논문96-1-1-09

로렌츠 시스템에 바탕을 둔 혼돈신호 덧씌우기

장 태 주, 송 익 호, 배 진 수, 김 홍 길

Chaotic Signal Masking Based on Lorenz System

Taejoo Chang, Iickho Song, Jinsoo Bae, and Hong-Gil Kim

요 약

이 논문에서는 로렌츠시스템에 바탕을 둔 신호 덧씌우기 방법의 한 구조를 생각하였는데, 이는 정보신호를 송신시스템 안으로 귀환시키는 구조이다. 이 방법은 수신쪽에서 정보신호를 정확히 복원하며 정보신호의 크기를 크게 할 수 있다. 모의 실험을 통하여 정보신호의 복원과 암호화 특성을 살펴보았다. 그리하여 다른 방식보다 성능이 뛰어남을 알 수 있었다.

Abstract

In this paper, we consider a signal masking structure based on the Lorenz system, which uses a feedback path of the information signal in the transmitter system. The scheme recovers the information signal exactly at the receiver, and can be used with increased amplitude information signal. The scrambling property of the scheme is also investigated by computer simulations, from which the performance is show to be better than that of the conventional method.

Ⅰ. Introduction

Chaotic signals are characterized by their high sensitivity to initial conditions : in other words, trajectories starting from arbitrarily close two points diverge exponentially with time, and quickly become uncorrelated. Recently, Carroll and Pecora [1] have shown that certain two chaotic systems achieve synchronization so that the two systems follow the same trajectory. It is also known that the synchronization is robust to perturbations of the synchronizing drive signal. These properties of chaotic signals suggest possible useful applications to spread spectrum and secure communications [2]. As a demonstration in secure communications, signal masking schemes based on Lorenz system and Chua's circuit have been considered in [3] and [4].

In the signal masking schemes using additive perturbation of the drive signal, the receiver cannot regenerate a perfect replica of the driver because of some synchronization error. In addition, the added signal level is usually limited to ensure reasonable recovery.

In this paper, we present a signal masking structure based on the Lorenz system, which is capable of alleviating the avove-mentioned difficulties by masking use of a feedback path of the information signal(a perturbation) in the transmitter system. We shall call the proposed scheme the *internal perturbation method.*

Ⅱ. Signal Masking Approaches

Signal masking based on the continuous-time chaos phenomenon is an analog scrambling method [6] for secure com-

한국과학기술원 전기및전자공학과
Dept. of Electrical Engineering, KAIST

munication, which prevents the information-bearing signal of a sender from being intercepted by any third party. In the transmitter, a large chaotic signal is added to the information-containing signal, thus the information signal is masked against the interceptor. At the receiver, a replica of the chaotic signal used in the transmitter is generated from the transmitted signal, which is then subtracted from the transmitted signal to recover the information signal.

Lorenz equations

$$\dot{x}=\sigma(y-x),$$
$$\dot{y}=r x-y-x z, \tag{1}$$

and

$$\dot{z}=xy-b z,$$

describing the chaotic signals x, y, and z, are used for a transmitter, where σ, γ, and b are positive real parameters. The corresponding receiver equations are give by

$$\dot{x}_r=\sigma(y_r-x_r),$$
$$\dot{y}_r=rx_t-y_r-x_t z_r, \tag{2}$$

and

$$\dot{z}_r=x_t y_r-b z_r,$$

where x_t is the transmitted signal used to drive the receiver. When $x_t=x$, the transmitter and the receiver are synchronized so that $x_r\to x$, $y_r\to y$, and $z_r\to z$, as $t\to\infty$ [3]. In signal masking, an information signal m is the perturbation signal, $p=m$. If the receiver is driven by x_t, then $x_r\approx x$, and m is recovered as $m=x_t-x_r$, as shown in Fig. 1. We call this scheme the *external perturbation method*. Recently, approximate analysis in signal masking and recovery has been done in [5] based on the external perturbation method. It is shown that the recovered signal m is improved by an additional lowpass filter.

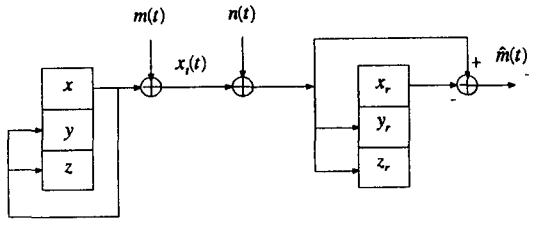


Fig. 1. Chaotic signal masking system(External perturbation method).

In the external perturbation scheme, the information signal level should be limited for synchronization, which is the main drawback of the scheme when noise is added to x_t. In addition the receiver cannot regenerate a perfect replica of the driver because of some synchronization error [5].

Ⅲ. The Internal Perturbation Method

Let us now consider a signal masking method, the internal perturbation method, which is capable of recovering the information signal at the receiver, and can be used with information signal amplitude larger than in the external perturbation method. In the internal perturbation method, the information signal is injected in the transmitter system, as shown in Fig. 2.

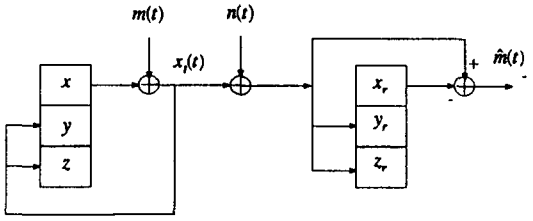


Fig. 2 Chaotic signal masking system(Internal perturbation method).

In Fig. 2, the transmitter is described by the three equations,

$$\dot{x}=\sigma(y-x),$$
$$\dot{y}=r x_t-y-x_t z, \tag{3}$$

and

$$\dot{z}=x_t y-b z,$$

where $x_t=x+m$ is the transmitted signal with m the information signal(a perturbation). The receiver can be described by the three equations in (2) as in external perturbation method.

The transmitter is the same as (1) if we replace x with x_t in the second and third equations of (3). Therefore we see without difficulty that (3) and (2) will asymptotically synchronize, as shown in Appendix. Thus, the message signal can be recovered exactly by subtracting x_r from x_t, i.e. $m=x_t-x_r=x_t-x=m$, at the receiver. Note that the synchronization is independent of the message signal m.

When some noise n is added to x_t during transmission, the internal perturbation method may have even better performance in recovering m compared to the external perturbation method for the same level of noise, since the internal pertur-

bation method can be used with information signal of high level.

Simulation results : As pointed out in [3], the transmitter and receiver need not be operating chaotically for synchronization to occur : for good signal masking, however, chaotic operation is desirable. We assume that the transmitter is in chaos when the system is unperturbed(i.e., when $m\equiv 0$ and $n\equiv 0$). We have investigated the transmitter dynamics by simulation, when a perturbation exists. In the simulations, we used the following set of equations for the amplitude and time-scaled variables with $\sigma=16$, $\gamma=45.6$, and $b=4$ when $m=0$, which are the same as in [3] :

$$\begin{aligned}\dot{x}&=G_T[16(y-x)],\\ \dot{y}&=G_T[45.6x_t-y-20x_tz],\\ \dot{z}&=G_T[5x_ty-4z],\end{aligned}\qquad(4)$$

where the time scaling factor $G_T=2505$.

We used (i) a dc signal and (ii) a speech signal, as m, In the simulation results, the recovered signal m is processed by an additional lowpass filter with cutoff frequency of 3kHz. Let us first consider the transmitter dynamics. When $m=m_0$ (dc signal), we have found that the system is in chaos for $|m_0|<m_c$, where m_C is observed to be between 0.5 and 0.6. When $|m_0|>m_c$, the trajectories keep moving to one of three non-zero fixed points, When $m=m_0+a\sin\omega t$, we observed that the dc level, m_0, plays the same role as m_0 in the case (i).

Next let us compare the two methods from the viewpoint of signal recovery and scrambling property. As is explained at the beginning of this section, the internal perturbation method recovers the information signal exactly at the receiver. In the external perturbation method, on the other hand, the recovered signal $\hat{m}$ is a distorted version of m. When the information signal is a speech signal shown in Fig. 3, the recovered signal using the internal and external perturbation methods under noise free environment are shown in Figs. 4 and 5, respectively, for $m(t)=2s(t)$.

When noise is present, and otherwise under the same condition as in Figs. 4 and 5, the recovered signals are shown in Figs. 6 and 7, respectively. We observe in general that the distortion decreases as the signal level increases in the internal perturbation method, in consrast to the external perturbation method. To compare the performance more formally, we used signal-to-noise ratio(SNR) and segmental SNR as objective measures, and the mean opinion scores (MOS) as a subjective measure [8]. The result is shown in Table 1. The values of

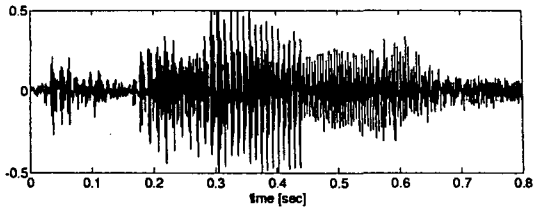


Fig. 3. A sample original speech $s(t)$

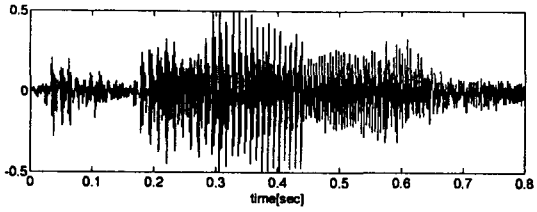


Fig. 4. The recovered signal when $n(t)\equiv 0$ and $m(t)=2s(t)$ with the internal perturbation method.

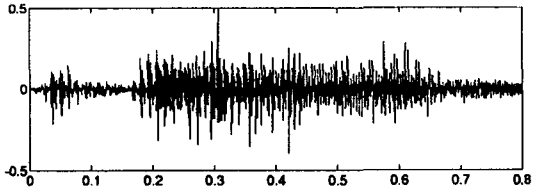


Fig. 5. The recovered signal when $n(t)\equiv 0$ and $m(t)=2s(t)$ with the external perturbation method.

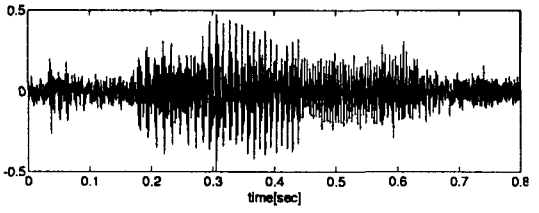


Fig. 6. The recovered signal when $n(t)\not\equiv 0$ and $m(t)=2s(t)$ with the internal perturbation method.

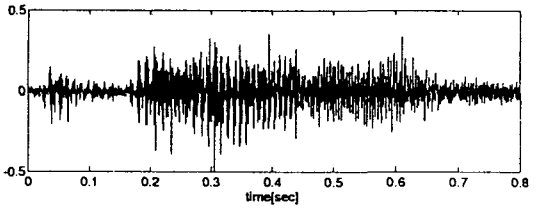


Fig. 7. The recovered signal when $n(t)\not\equiv 0$ and $m(t)=2s(t)$ with the external perturbation method.

the SNR and segmental SNR turn out to be similar.

Table 1. Recovered signal comparison

	the internal perturbation		the external perturbation	
amplitude	SNR(dB)	MOS	SNR(dB)	MOS
0.5	12	4	10	3
1.0	23	3	9	1
2.0	31	2	3	1

In order to see the scrambling property, we have investigated the average power spectrum of the transmitted signal x_t. When the information signal is a speech signal, we investigated that the internal and external perturbation methods seem to produce similar spectrum.

Ⅳ. Concluding Remarks

A new signal masking structure is considered based on Lorenz system : in the proposed method, the information signal is injected in the transmitter system. The proposed method recovers the information signal exactly at the receiver, and can be used with information signals of increased amplitude. The scrambling properties are shown by simulations. It may be worth to investigate further properties of the transmitter dynamics in more detail for a practical application. It should be mentioned that a general approach for constructing chaotic synchronized dynamical systems has been proposed recently [9], from which the structure of the internal perturbation method may also be derived if we choose an appropriate function.

Acknowledgements

This research was supported in part by the Ministry of Information and Communications under a Grant from the University Basic Research Fund, for which the authors would like to express their thanks.

Appendix
Proof of Synchronization

We denote the transmitter and receiver state variables by the vector $x=(x, y, z)$ and $x_r=(x_r, y_r, z_r)$, resectively. Define the dynamical errors $e=(e_1, e_2, e_3)=x-x_r$. Then assuming that the transmitter and receiver coefficients are identical, the error dynamics is given by

$$\dot{e}_1=\sigma(e_2-e_1), \tag{5}$$

$$\dot{e}_2=-e_2-x_1e_3$$

$$\dot{e}_3=x_1e_2-be_3$$

Consider the function,

$$E(e, t)=\frac{1}{2}(\frac{1}{\sigma}e_1^2+e_2^2+e_3^2) \tag{6}$$

The function E is obviously positive definite when $\sigma>0$. We get

$$\dot{E}=\frac{1}{\sigma}e_1\dot{e}_1+e_2\dot{e}_2+e_3\dot{e}_3 \tag{7}$$

$$=e_1e_2-e_1^2-e_2^2-be_3^2$$

$$=-(e_1-\frac{1}{2}e_2^2)^2-\frac{3}{4}e_2^2-be_3^2 \tag{8}$$

Hence, $\dot{E}\leq 0$ with equality only if $e=0$. Therefore E is a Liapunov function, and thus $e(t)\rightarrow 0$ as $t\rightarrow\infty$.

Furthermoer, it can be shown that the rate of synchronization is exponentially fast using the similar procedure as in [3].

References

[1] T. L. Carroll and L. M. Pecora, "Synchronizing chaotic circuits," *IEEE Trans. Circuits Syst.*, vol. 38, pp.453-456, Apr. 1991.

[2] A.L. Oppenheim, G.W. Wornell, S.H. Isabelle, and K.M. Cuomo, "Signal processing int the context of chaotic signals," *Proc. IEEE ICASSO*, pp.117-120, San Francisco, CA, USA, Mar. 1992.

[3] K. M. Cuomo, A. V. Oppenheim, and S. Strogatz, "Synchronization of Lorenz-base chaotic circuits with application to communications," *IEEE Trans. Circuits Syst.- Ⅱ : Analog, Digital Signal Process.*, vol. 40, pp. 626-633, Oct. 1993.

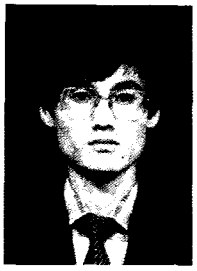
[4] LJ. Kocarev, K. S. Halle, K. Eckert, and L. O. Chua, "Experimental demonstration of secure communications via chaotic synchronization," *Int. J. Bifurcation, Chaos*, vol. 2, pp. 709-713, Sept. 1992.

[5] K. M. Cuomo, A. V. Oppenheim, and S. Strogatz, "Robustness and signal recovery in a synchronized chaotic system," *Int. J. Bifurcation, Chaos*, vol. 3, pp. 1629-1638, Dec. 1993.

[6] W. Diffie and M. E. Hellman, "Privacy and authentication : An introduction to cryptography," *Proc. IEEE*, vol. 67, pp. 397-472, Mar. 1979.

[7] S. M. Cox, "The transition to chaos in an asymmetric perturbation of the Lorenz system," *Physics Letters A*, vol. 144, pp. 325-328, Mar. 1990.
[8] N. S. Jayant and Peter Noll, *Digital Coding of Waveforms*, Prentice-Hall, Englewood Cliffs, NJ. 1984.
[9] L. Kocarev and U. Parlitz, "General approach for chaotic synchronication with application to communication," *Physical Rev. Lett.*, vol. 74, pp. 5028-5031, June 1995.

저 자 소 개



張 泰 株
1960년 4월 20일생
1982년 2월 : 울산대학교 전기공학과 졸업 (공학사)
1990년 2월 : 한국과학기술원 전기및전자공학과 졸업 (공학석사)
1994년 3월 ~ 현재 : 한국과학기술원 전기및전자공학과 박사과정
* 주관심 분야 : 정보이론, 통신이론

宋 翊 鎬
1960년 2월 20일생
1978년 3월 ~1982년 2월 : 공학사(준최우등), 전자공학과, 서울대학교
1982년 3월 ~1984년 2월 : 공학석사, 전자공학과, 서울대학교
1984년 1월 ~1985년 8월 : 공학석사, 전기공학과, Univ. of Pennsylvania
1985년 9월 ~1987년 5월 : 공학박사, 전기공학과, Univ. of Pennsylvania
1987년 3월 ~1988년 2월 : 벨 통신연구소 연구원
1988년 3월 ~1991년 8월 : 한국과학기술원 조교수
1991년 9월 ~현재 : 한국과학기술원 부교수
1995년 2월 ~현재 : 한국통신학회 논문지 편집위원
*주관심 분야 : 통계학적 신호처리, 신호검파, 스펙트럼 추정, 이동통신

裵 鎭 秀
1972년 3월 11일 서울생
1990년 2월 : 경기과학고등학교 조기졸업 (우등)
1993년 2월 : 공학사, 한국과학기술원 전기및전자공학과 (최우등, 3년 조기졸업, 전체차석)
1995년 2월 : 공학석사, 한국과학기술원 전기및전자공학과
1995년 3월 - 현재: 한국과학기술원 전기및전자공학과 박사과정 재학중
*주관심 분야 : 신호검파, 추계적과정, 신경회로망, 통신이론, 해석학, 대수학

金 洪 吉
1972년 7월 20일생
1995년 2월 : 한양대학교 전자통신공학과 졸업 (공학사)
1995년 3월 ~ 현재 : 한국과학기술원 전기 및 전자공학과 석사과정
*주관심 분야 : 검파이론